Security Architecture for Wireless Ad hoc Networks

Stefaan Seys

K.U.Leuven
Department Electrical Engineering (ESAT)
Kasteelpark Arenberg 10
B-3001 Leuven (Heverlee)
telephone: +32 (0)16 32 11 34, fax: +32 (0)16 32 19 86
stefaan.seys@esat.kuleuven.ac.be

1 INTRODUCTION

This paper summarizes three main technical contributions of our PhD project[1] entitled "Security Architecture for Wireless Ad hoc Networks". Ad hoc networks are a new paradigm of wireless communications for wireless hosts or nodes. In an ad hoc network there are is no supporting infrastructure like base stations, access points or wireless switching centers. An ad hoc network can be established as soon as two or more nodes are within each other's transmission range. Nodes within range communicate directly, while nodes further apart rely on other nodes to relay messages for them. If the nodes in the network are mobile, then the topology of the network frequently changes. Military operations are still the main application of ad hoc networks, but civilian applications include smart homes, patient monitoring while they and the staff roam the hospital, environmental control, etc.

Security is as important in ad hoc networks as it is in more traditional networks like the Internet. Sensitive data should be protected from malicious eavesdroppers and network services should only be provided to eligible users.

1.1 SECURITY CHALLENGES IN AD HOC NETWORKS

Providing adequate security measures for ad hoc networks is a challenging task.

First, wireless communications are easy to intercept and difficult to contain. Next to this it is easy to actively insert or modify wireless messages. This means that unprotected wireless networks are open to a wide range of attacks, including node impersonation, message injection, loss of confidentiality, etc.

Secondly, in many situations the nodes may be left unattended in a hostile environment. This enables adversaries to capture them and physically attack them. Proper precautions (tamper resistance) are required to prevent attackers from extracting secret information from them. Even with these precautions, we cannot exclude that a fraction of the nodes may become compromised. This enables attacks launched from within the network.

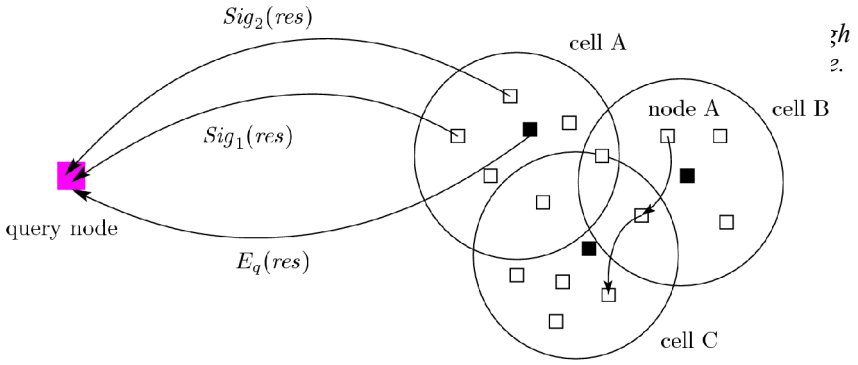
Thirdly, the dynamic topology and the absence of a supporting infrastructure renders most of the existing cryptographic protocols useless as they were not developed for this dynamic

[1] This work was funded by a research grant of the Flemish Institute for the Promotion of Industrial Scientific and Technological Research (IWT).

environment. Any security solution with a static configuration would not suffice. Security mechanisms should be able to adapt on-the-fly to these changes in topology.

Fourthly, many wireless nodes will have a limited energy resource (battery, solar panel, etc.). This is particularly true in the case of ad hoc sensor networks. Security solutions should be designed with this limited energy budget in mind.

Finally, an ad hoc network may consist of thousands of nodes. Security mechanisms should be scalable to handle such a large network.



2 POWER CONSUMPTION OF DIGITAL SIGNATURES

We have evaluated the power consumption of different digital signature schemes. We compare the computational cost of the Elliptic Curve Digital Signature Algorithm (ECDSA) with the cost of digital signature schemes based solely on efficient symmetric cryptographic techniques. In these power consumption evaluations, we take into account all aspects of using these schemes in wireless environments: energy consumption of key generation, signing, verification and the communicational cost of sending and receiving the necessary data (the signatures themselves, but also the public keys and the necessary data to authenticate these keys).

The digital signature schemes based on symmetric cryptographic techniques we evaluated are the Lamport-Diffie one-time signature scheme and the HORS (Hash to Obtain Random Subset) signature scheme by Reyzin and Reyzin. Both these schemes are one-time signature schemes, meaning that the private key can only be used once to create a signature. Therefore, in order to make these schemes practical, an efficient authentication mechanism for the public keys is required. We have evaluated the cost of two authentication mechanisms: Merkle trees and one-way chains. Summarizing our results we can say that (1) one-way chains are most efficient for signature verification, (2) ECDSA and both one-time schemes using Merkle trees are most efficient for signature generation, and (3) ECDSA is the best candidate concerning communicational cost (due to the short signatures and the fact that the private key can be used multiple times). We also conclude that the most demanding task is signature generation, then verification and finally communications.

3 DYNAMIC KEY MANAGEMENT

We have developed a key management scheme for dynamic ad hoc networks. Our scheme builds on existing key pre-distribution schemes in order to bootstrap the process. A key pre-distribution scheme distributes a set of secret keys in every node before these nodes are deployed in the field. Once the nodes are deployed, the pre-distribution scheme can provide guarantees of two nodes sharing a secret key with a particular fraction of its neighbors (this fraction is one of the parameters of the key pre-distribution scheme). In our scheme, the first step is to enlarge this fraction by using trust relationships (node A has shares a key with B,

and B with C, then A can use B to setup a key with C). This way, a node can establish a shared secret key with every node within its neighborhood. In order to make the scheme dynamic, we trigger this neighborhood discovery process every ΔT milliseconds. As long as two consecutive neighborhoods of a node overlap, the nodes in this overlap can be used to establish keys with all the new nodes in the new neighborhood (Fig. 1 shows node A moving through the network). In order to improve the security of the scheme, we use multiple trusted paths to establish these shared secrets. We show how our scheme can be build on top of a well known routing scheme for ad hoc networks: Dynamic Source Routing (DSR); and how DSR itself can be secured using the keys established with our scheme. Finally, we have evaluated the total overhead of our scheme using a network simulator we have written in Java.

4 EFFICIENT GROUP AUTHENTICATION

We propose a mechanisms that allows query nodes in a sensor network to securely pull data from the sensor nodes. Two important issues are tackled in this work: (1) multiple nodes have to cooperate in order to digitally sign a message, and (2) only efficient operations are required (at least for the low-power sensor nodes).

The RSA public key cryptosystem comes in two flavors: a signature scheme and an encryption scheme. Both algorithms require a private key and a corresponding public key. In order to sign a document, one uses his private key (known only to the signer). Other users can verify the signature using the corresponding public key (publicly available). For encryption the use of keys is inversed: in order to encrypt a message, one uses the recipients public key, while the recipient uses his private key to decrypt the cryptogram. In both cases the public operation (signature verification and encryption) is very efficient, while the private operation is rather inefficient . In our scheme the sensor nodes only have to perform the public operations.

In order to support authentication from the nodes to the query node, we have adapted an existing one-time signature scheme. This adapted scheme (based on efficient symmetric cryptographic algorithms) enables multiple nodes to cooperatively sign (authenticate) a message. Figure 1 shows how the nodes in cell A cooperate to sign a response to the query node. The manager node (black) transmits the encrypted response, while the other nodes in the cell transmit a partial signature on this response. Our design is flexible in that it allows some partial signatures to be lost or corrupted and still provide a valid signature on the message. It also allows to reconfigure the group size of the nodes that cooperate to sign a message. Finally, in our scheme the nodes actually divide the load of signing a message, i.e., a partial signature requires less effort than signing a complete message.

5 CONCLUSIONS

In this paper we have summarized three techniques that were developed during the course of our PhD project “Security Architecture for Wireless Ad hoc Networks”. This PhD project focuses on providing security in the highly dynamic and power-restrained environment of wireless ad hoc networks. A first contribution evaluates power consumption of different digital signature schemes, next we present a dynamic key management scheme and finally we propose a novel authentication scheme.